CÓDIGOS MALICIOSOS

EXÉRCITO BRASILEIRO

Produção:

COM D CIBER

E NA D CIBER

Códigos maliciosos (*malware*) são usados como intermediários para prática de golpes, realização de ataques e envio de spam. A melhor prevenção é impedir sua infecção inicial, pois nem sempre é possível reverter ações já feitas ou recuperar dados vazados ou perdidos.

Antivírus (*antimalware*) podem ajudar a detectar, prevenir a infecção e/ou remover *malware*. No entanto, para serem efetivos contra a infinidade de variantes e novos *malware* que surgem todos os dias, precisam de **atualização contínua**.

MANTENHA OS SISTEMAS E APLICATIVOS SEMPRE ATUALIZADOS

Códigos maliciosos costumam explorar vulnerabilidades em sistemas e aplicativos para infectarem os dispositivos e se propagarem. Aplicar correções de segurança pode evitar que seus dispositivos sejam infectados e usados por atacantes.

» Instale atualizações regularmente

» Ative a atualização automática, sempre que possível

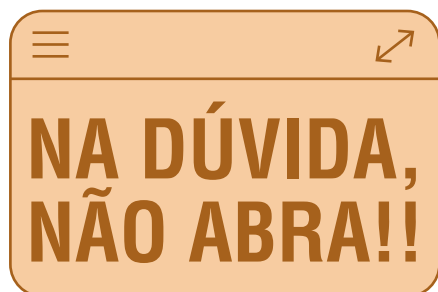
» Reforce os cuidados, caso seu dispositivo já tenha sido infectado, para que não ocorra novamente

NÃO CLIQUE EM TODOS OS LINKS QUE RECEBE

Alguns links podem ser usados para direcionar os usuários para páginas contendo códigos maliciosos, visando infectar e ganhar acesso aos dispositivos. Os atacantes empregam vários truques para induzir os usuários a clicarem nestes *links*, como enviá-los de contas falsas ou invadidas.

DESCONFIE SEMPRE DE ARQUIVOS ANEXOS

Os atacantes podem utilizar e-mails com anexos maliciosos, sobre temas que despertam o interesse e a curiosidade dos usuários, para instalar *malware*.

- Cheque o arquivo com antivírus, antes de abri-lo.

BAIXE APLICATIVOS SOMENTE DE LOJAS OFICIAIS

Existem aplicativos para celulares e tablets que se passam por legítimos, mas que na verdade possuem códigos maliciosos.

As lojas oficiais costumam ter políticas mais rígidas e mecanismos mais rápidos de exclusão destes aplicativos, quando detectados.

- Nunca instale aplicativos recebidos via mensagens ou links
- Antes de instalar, confirme o nome do aplicativo e se o desenvolvedor é mesmo quem deveria ser

Os dados armazenados em seus dispositivos podem ser perdidos pela ação de códigos maliciosos como *ransomware*. Ter cópias permite recuperá-los, reduzindo os transtornos.

- Faça cópias periódicas de seus dados

- Programe seus *backups* para serem feitos automaticamente, sempre que possível

UTILIZE AUTENTICAÇÃO FORTE

Códigos maliciosos podem capturar e expor suas senhas. Para se **prevenir** contra vazamentos e **acessos indevidos**, é importante proteger suas contas com formas **adicionais de autenticação**.

» Use verificação em duas etapas, sempre que possível

» Não repita senhas
  • uma senha vazada pode levar à invasão de outras contas

» Armazene suas senhas de forma segura
  • não salve-as no navegador

» Troque **imediatamente** suas senhas se desconfiar que elas vazaram ou foram usadas em um dispositivo infectado

USE A CONTA DE ADMINISTRADOR SOMENTE QUANDO FOR NECESSÁRIO

- » Um *malware* consegue fazer no dispositivo o mesmo que o usuário que o ativou, e terá acesso irrestrito se a conta usada for de **administrador**. Criar contas padrão e usá-las no cotidiano, ajuda a limitar as ações dos códigos maliciosos

- » Essa recomendação baseia-se em um princípio de segurança conhecido como “**privilégio mínimo**” e visa evitar danos por uso não autorizado ou erros

AJA RAPIDAMENTE EM CASO DE SUSPEITAS DE PROBLEMAS

Abriu um arquivo ou clicou no link de um e-mail e depois descobriu que era um *malware*? Seu dispositivo está estranho?
AJA RAPIDAMENTE!

» Use **imediatamente** o antivírus que estiver instalado ou empregue outras opções disponíveis online

» Reinicie o dispositivo, pois isto pode ser suficiente para remover o *malware*, em casos onde ele fica apenas na memória

» Se não for possível remover o *malware* ou os sintomas persistirem, **reinstale o sistema** ou **restaure as configurações de fábrica**

» Altere as senhas dos serviços que costuma acessar do dispositivo infectado.

Reinstalar o sistema ou restaurar as configurações de fábrica, apesar de trabalhosas, são as **soluções mais recomendáveis** pois nem sempre é possível ter certeza de que o código malicioso foi totalmente excluído.

CONHEÇA SEUS PRINCIPAIS INIMIGOS

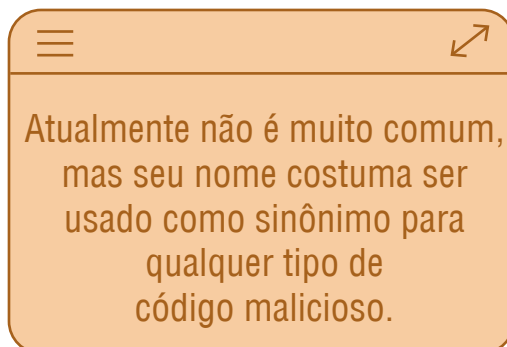
Códigos maliciosos (*malware*) são programas que executam ações danosas e atividades maliciosas. São muitas vezes chamados genericamente de "vírus", mas existem diversos tipos com características próprias. Conhecer estas características ajuda a identificar comportamentos estranhos no dispositivo e a entender as melhores maneiras de repará-lo. Também permite estimar o tipo de dano e como atuar, pois alguns furtam dados, outros cifram seus dispositivos e outros podem ser usados para fraudes.

Conheça aqui alguns dos principais tipos de códigos maliciosos.

VÍRUS

Torna-se parte de programas e arquivos.

Propaga-se enviando cópias de si mesmo por e-mails e mensagens

Atualmente não é muito comum, mas seu nome costuma ser usado como sinônimo para qualquer tipo de código malicioso.

RANSOMWARE

Torna inacessíveis os dados armazenados no dispositivo, geralmente usando criptografia, e **exige pagamento de resgate** para restabelecer o acesso ao usuário e não vazar os dados.

Após infectar o dispositivo, exibe uma mensagem informando ao usuário o procedimento a ser seguido para restabelecer o acesso, incluindo:
valor do resgate (geralmente em criptomoedas), prazo para pagamento, identificação do dispositivo do usuário e forma de contato com o atacante, como um link ou endereço de e-mail.

SPYWARE

Projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

São tipos específicos de *spyware*:

KEYLOGGER

Captura e **armazena as teclas digitadas**. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

SCREENLOGGER

Armazena a posição do cursor e a tela apresentada no monitor, ou a região que circunda determinada posição, nos momentos em que o mouse é clicado. Usado para capturar **teclas digitadas em teclados virtuais**.

ADWARE

Projetado para apresentar **propagandas indesejadas** na tela de seu dispositivo.

STALKERWARE

Projetado para **espionar o dono do dispositivo**, que não autorizou e não sabe que tal código está instalado. As informações coletadas são enviadas para quem o instalou ou induziu sua instalação (nesse caso, chamado *stalker*).

TROJAN (CAVALO DE TROIA)

Além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e **sem o conhecimento do usuário.**

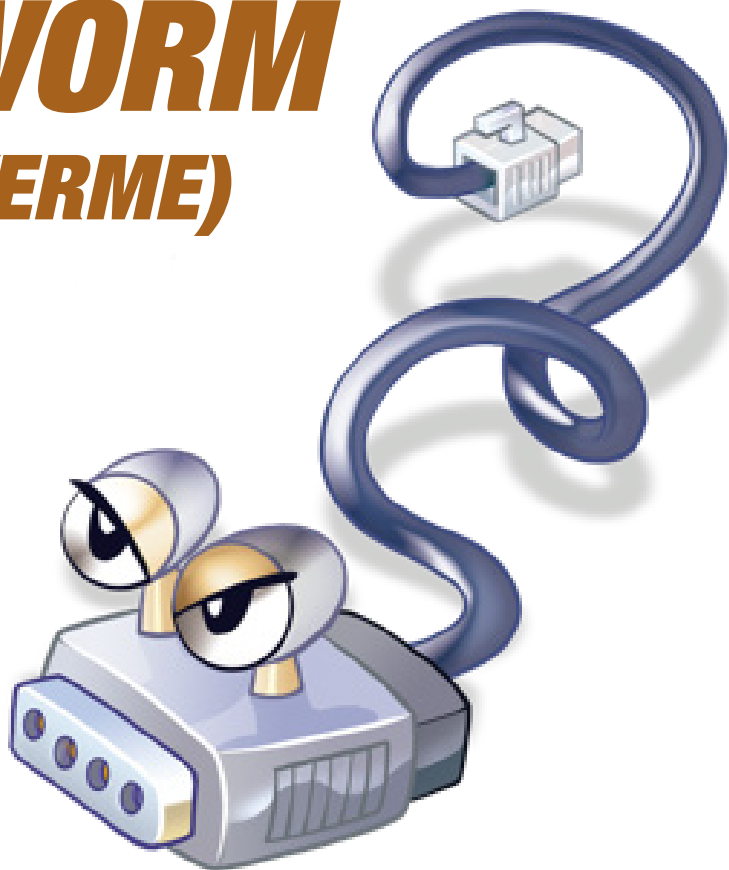
É como se fosse uma **porta acessível** (porta dos fundos), que permite o retorno do invasor a um dispositivo comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

Pode ser incluído pela ação de outros códigos maliciosos que tenham infectado o dispositivo ou por atacantes que exploram vulnerabilidades no sistema ou aplicativos para invadi-lo.

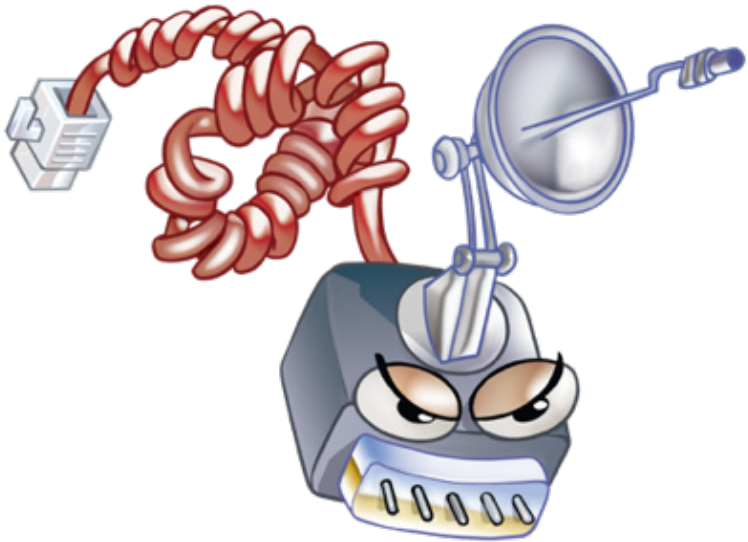
REMOTE ACCESS TROJAN (RAT)

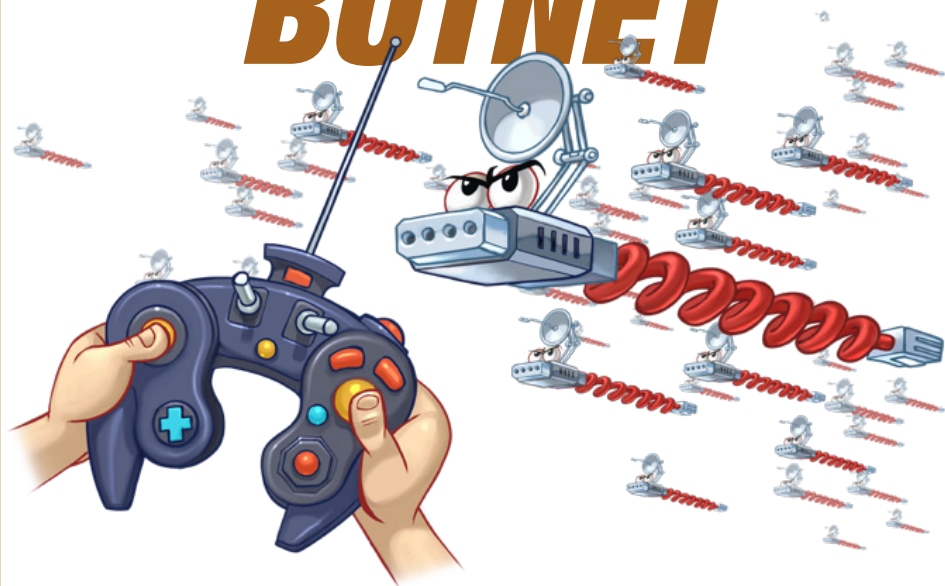
É um *Trojan* de Acesso Remoto, que permite a um atacante acessar remotamente um dispositivo infectado de forma direta e interativa.

Combina as características de *trojan* e *backdoor*, pois tenta enganar o usuário, assim como o trojan, e permite que um atacante **acesse remotamente** o dispositivo e execute ações como se fosse o usuário, assim como o *backdoor*.

WORM (VERME)

Propaga-se automaticamente pelas redes, explorando vulnerabilidades nos sistemas e aplicativos instalados e **enviando cópias de si mesmo** de dispositivo para dispositivo.

É responsável por **consumir muitos recursos**, devido à grande quantidade de cópias de si mesmo que costuma propagar e, como consequência, pode afetar o desempenho de redes e a utilização de dispositivos.

BOT (ROBÔ)

Similar ao *worm*, possui mecanismos de comunicação com o invasor, que permitem que ele seja **remotamente controlado**. *Bot* ou *Zumbi* são os nomes dados aos dispositivos infectados por esse *malware*.

BOTNET

Rede formada por **inúmeros dispositivos zumbis**. Permite potencializar as ações danosas executadas pelos *bots*. Quanto mais zumbis participarem da botnet e quanto maiores forem as capacidades de conexão e processamento desses zumbis, mais potente ela será.

Algumas das ações executadas por meio de *botnets*:

» ataques de negação de serviço (DDoS);

» propagação de *malware* (inclusive do próprio *bot*);

» coleta de informações pessoais;

» envio de *spam*; e

» mineração de criptomoeda.

ROOTKIT

Conjunto de programas e técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um dispositivo comprometido.

O termo *rootkit* não indica que os programas e as técnicas que o compõem são usadas para obter acesso privilegiado a um dispositivo, mas sim para mantê-lo. Origina-se da junção das palavras "*root*" (conta de superusuário ou administrador do dispositivo em sistemas Unix) e "*kit*" (conjunto de programas usados para manter os privilégios de acesso dessa conta).

SCAREWARE

Usa técnicas de **engenharia social** para assustar e enganar o usuário, fazendo-o acreditar na existência de um problema de segurança em seu dispositivo e oferecendo uma solução para corrigi-lo, mas que, na verdade, poderá comprometê-lo.

Exemplos de *scareware* são janelas de pop-up que informam que o dispositivo está infectado e, para desinfetá-lo, faz-se necessário instalar um **(falso) antivírus**, que é na verdade um código malicioso.

SAIBA MAIS
Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais fascículos da Campanha de Conscientização Cibernética no site EB.MIL.BR